Final Thesis

Table of Contents

Final thesis **1**
Abstract 1
INTRODUCTION 1
You Are Being Tracked 1
A Tracking Example 1
Nothing To Hide 1
Remembering The Advise 1
The Browser 2
A Website 2
Webpages Come In Parts 2
3rd Parties 2
Some Statistics About 3rd Party Involvement 3
YOUR DATA 3
What Your Browser Tells About Himself 3
Ip Address 3
Cookies 3
Tracking Cookies And Web Beacons 4
Tracked By Facebook Without Having A Facebook Account 4
Tracked By Google In The Name Of Marketers 4
Other Track Methodologies 4
THEIR MONEY 5
Targeted Advertisement 5
Targeting Companies 5
Retargeting Companies 5
Monitoring Companies 5
Insurance Companies 6
Banks 6
Employment Agencies 6
Rogue Employees 6
Many More Possibilities 6
GOOD REASONS TO TRACK PEOPLE 6
Machine Learning At Google 6
Machine Learning Should Be Anonymous 7
Science 7
Data Journalism 7
Application Programming Interface 7
Attention Economy 8
BAD REASONS TO TRACK PEOPLE 8
Demystifying The User Experience 8
Hit And Long Tail Markets 8
Examples Of Long Tail Companies 9
Making A Longer Tail 10
Create Access To The Tail 10
Filtering The Tail 11
How Targeted Advertisement Works 12
A Different Realm 13
Failure To Deliver A Good User Experience By Google 13
Retargeting And Use Experience 13

Table of Contents

Final thesis

Successes Are Biased....13
PAYING WITH PRIVACY....13
No Such Thing As A Free Lunch....13
Advertisement Cross Subsidy....14
Freemium....14
The Value Of Privacy....14

Final thesis

Word estimate: 5887
Click here to go to the index.

Abstract

This thesis explores how people are being tracked online, why this may be a problem and why the user is not benefited by tracking in anyway. I also discuss how to prevent tracking from happening and what possibilities companies have to make money without tracking consumers. My project attached to this thesis is an attempt to make clear which risks and changes are involved concerning the huge amount of data that gets generated around our personas in a playful manner.

INTRODUCTION

You Are Being Tracked

When you are online it gets tracked, among other things, which sites you visit and which things you buy. It happens to all of us if you don't take precautions. This information is saved for about six months (in some cases longer) and gets used to make money by different parties. This thesis will discuss in which ways information about your behavior online is valuable and how falls into the hands of who is interested in it.

A Tracking Example

The fact that you are being tracked is problematic when sensitive information is disclosed to parties who were not supposed to have that information. This could happen when you do your groceries online. Insurance companies may keep track of what you eat and adjust your fee, because your eat habits indicate a heightened change for diabetes.

Nothing To Hide

You may think that you donâ t have anything to hide even when you've read about some examples. Are your friends and family in the same position? Will you have something to hide as you get older and your medical data becomes more valuable to insurance companies? Aren't there any ways imaginable in which information about you can be used against your interest, although it doesn't happen right now? Surely one of the answers to these questions is yes. In that case it's better to live in a society where you donâ t have to worry about whether sensitive information gets revealed or not.

Remembering The Advise

I have made a list of incentives which you could follow to better protect yourself from unwanted information disclosure. However a rule, without an explanation of why that rule is important, is just another rule. Such rules are likely to get broken! Thatâ s why I want to explain you in simple terms why these rules are important and how they affect your privacy. It will take a little more effort to understand this than to read the bullet point list of incentives. Then again once you understand the incentives you can better protect not only yourself but also others who are in need for it and havenâ t red this thesis themselves.

The Browser

When you visit a webpage on a website you're using a computer program that is called a browser. Examples of browsers are Internet Explorer, Firefox, Chrome, Safari and Opera. From these browsers Firefox and Opera are the most independent browsers and considered best at protecting your privacy online.

A Website

A website is a collection of webpages. For now lets think about webpages as being files, which they used to be in the early days of the internet. All webpage files of a website reside on a computer, which is part of the internet infrastructure. As soon as you click on a link to visit a webpage your browser makes connection with a computer which stands in a room like you see below:

Many powerful computers are stored in those things that look like fancy refrigerators on the image. Together these computers are a part of the internet. When you see a webpage in your browser it has been send to your browser by one of these computers, which are called servers. Think about these computers as the devices that serve you the web pages your browser requested for when you click links.

Webpages Come In Parts

Your browser receives an entire webpage in parts. The first part, which usually contains all text on the webpage, will also indicate to a browser where it can find other parts. These additional parts may be images, video or audio, that are on the webpage you're visiting. Since these parts are often essential to the look of the webpage your browser will download these parts without checking if they are necessary.

3rd Parties

Parts of a website can be located on the same computer as the webpage your visiting (a website logo for instance), but they could also be coming from completely different computers. Whenever webpage parts don't originate from the website being visited we speak of â 3rd partiesâ being involved with that webpage.

Think for instance about Facebooks â like itâ buttons or Youtubes video players, but also banners and commercials. These media are retrieved from Facebook, Google or another media company and never from the website you're visiting. When 3rd party computers are involved to construct a webpage these companies don't only provide webpage parts, but they also have the opportunity to record that you visited webpage X on website Y.

Some Statistics About 3rd Party Involvement

75% of more than 100 popular websites reveal information about their visitors to 3rd parties. 50% of these websites makes uses of unique identifiers stored in tracking cookies. Other things these websites share with 3rd parties are full names, email addresses, home addresses and information coming from your browser. The amount of 3rd parties in existence is somewhere around a thousand. It's not uncommon for a single person to be tracked by a 100 companies.

YOUR DATA

What Your Browser Tells About Himself

Whenever you are visiting a website where a 3rd party is involved (this happens often!) your browser tells a few things to this 3rd party. It depends on the browser what gets told exactly, but usually it will tell which browser you are using and if you are on a Mac, Windows, Android or other kind of computer. It may also reveal your language setting and which webpage you were visiting before. This information combined already tells a lot about you, because only a few people will share exactly the same information with 3rd parties. This makes you identifiable. The really revealing information that gets collected however is the IP address in combination with the content of a so called cookie file.

Ip Address

When your the-browser connects to a server for a part of a webpage this computer does need to know where to send the part of the webpage to. To inform websites where you want the webpage parts to be delivered your browser specifies your IP address (Internet Protocol Address). This address that basically functions like your post address is given to you by your internet provider. Any part of a webpage that a browser asks for gets delivered at this address where the browser will put them together to form a whole. Sometimes you share your IP address with the people you live with and it can also happen that you get a partially new address every time you turn on your computer (depends on your internet provider). In general the IP address will limit the size of the group of people who may have asked for the webpage significantly and thus comes very close to identifying you.

Cookies

Cookies are files that are automatically stored on your computer, by your browser, when you are visiting websites. The content of a cookie file is determined by the server responsible to deliver some part of a website you're visiting. So apart from getting a part of a website you also get arbitrary information to be stored by your browser in a cookie file. When your browsers asks for any other webpage part on the same server, your browser will tell that server what it has stored in his cookie file previously. The content of a cookie file might be the products youâ ve been shopping for so far on a certain website for instance. When you visit the paying webpage of the webshop the content of the cookie file gets transferred to the website. In this case a correct bill may be generated from the cookie file information, since it contains all products you shopped for. The generated bill is then shown on the paying webpage. Cookie files are also used to login to a website and

to save your preferences on a website.

Tracking Cookies And Web Beacons

Tracking cookies are a specific kind of cookie that hold the web equivalent to your social security number. Like with any content of a cookie this identifying number gets send over to a server whenever you visit a webpage that features a webpage part stored on that particular server. This means that if a certain image or other part of a website is used on lets say a million pages, your travel path between those pages gets tracked precisely, because your browser unknowingly sends along the identifying number which is unique for you, every time you download the image or another webpage part, which is swarming over the internet.

Often the webpage parts used in this way are invisible elements, that don't add to the user experience, but only exist to allow for tracking. This kind of webpage part is referred to as being a web beacon. [[[seperate page??]]]

Tracked By Facebook Without Having A Facebook Account

Since Facebook's like button is present on so many webpages. Facebook is enabled to track people over the web outside of Facebook itself. You don't even need to have an account with Facebook to get tracked, nor do you need to click the buttons in order for it to work.

Facebooks â like itâ button is a web beacon. Their sheer presence is enough to tell Facebook you've been visiting a page. The â like itâ button is separately retrieved from a computer owned by Facebook and not from the website you were originally visiting. This indicates to Facebook that you visited that site. Your identity is established by Facebook through tracking cookies which act as a kind of passport, that gets shown to Facebook whenever a webpage holds a â like itâ button. If you are registered with Facebook that is a bonus. Your name and everything else you share on Facebook will get related to the online passport as well as your web visits.

Tracked By Google In The Name Of Marketers

A service by Google called Google Analytics is used by marketers of various companies who want to know which pages of their website get viewed most often, how long visitors are staying, where they point there mouse and which links they click to leave the page. Apart from this your browser tells a few other things, which are made available to the marketers also. Google Analytics is active on about 80% of all websites.

Google Analytics makes use of tracking cookies and web beacons, which report to Google. Through Google graphs about visitors are generated for marketers showing which marketing actions are effective and which arenâ t. Currently Google states that they are not allowed to interpret the data coming from Google Analytics for themselves. However they have begun a program, where you have to apply for, called Screenwise. If you do apply Google will fetch the Google Analytics kind of information from all websites you visit and not only the ones where Google Analytics is installed by marketers. In return for doing this you get 25 dollar. Itâ s possible that in the long run Google will use the algorithms, that they may be using with Screenwise, upon data collected by Google Analytics. Their recent change in privacy policy could be interpreted as a step in that direction.

Other Track Methodologies

Spyware is a special kind of virus specifically designed to track people. This can be information on how you use your computer, but they may also see what your webcam is filming.

The browser on your mobile phone can send additional information about you, for instance your Google account ID, when you're using an Android phone. This makes everything you do online with a smartphone easily connected to your full name and other personal information.

Not only websites can have beacons, emails have them as well. Through these beacons spammers can focus their campaigns upon people who open their emails.

These days a lot of people don't directly go to a website, but they go to it through a search engine. Instead of typing a web address in the browser, people search for the name of the site. If you use the web this way, then the search engine will know what places you visit. What people don't realize is that some search engines save this information, which means your online history may become public one day.

Another major problem with going online through search engines is that the search engines will often inform the websites what you've been searching for. What if a medical information website run by an insurance company, knows you've been searching for cancer? In the next section I'll go deeper into how people can earn money by tracking others.

[[[hackers?]]]

THEIR MONEY

Targeted Advertisement

The main reason where cookies and web beacon information is used for is targeted advertisements. You see this kind of commercials everywhere online these days. Through web beacons it is known to 3rd parties which online shops you've been visiting and what you bought. When those parties can show commercials on a site you're visiting, because the webpage part containing the advertisements is coming from their computers. Then they will show advertisements that fit the information they received from the beacons. If you've ever visited a shoe shop online for instance, but didn't buy anything, changes are great that you get a lot of shoe commercials for weeks to come.

Targeting Companies

These companies create a profile about you, based on what they now about the content of the webpages you visited in the past. Whenever possible they'll show you ads that in their opinion are related or relevant in relation to the content you've been browsing so far. This may be quite far off. If I have a tooth pain, and I visited a forum about that, I may get commercials about toothbrushes. It has to do with teeth, but it's not the solution I'm searching for probably.

Retargeting Companies

Companies from this kind are mostly active in and around webshops. They'll monitor your buying behavior and when you don't buy they'll show you commercials from the products you haven't bought yet. Of course it is their hope that this time you'll get persuaded and make a buy online from the company they are working for.

Monitoring Companies

These companies are working like accountants. It would be easy for a retargeting company to say that they've been showing all kinds of commercials about products that users didn't buy before, but how does the seller of

these products know that this is true? They'd have to track people themselves in order to know that these companies are not conning them in some way. Instead of tracking people themselves they leave it to specialized companies who monitor the monitors by monitoring you.

Insurance Companies

Insurance companies are already looking at how they may use tracking data to predict risks concerning you. For instance they try to tell what the change is you get depressed by looking at which sites about food you visit. If they deem certain risks very high they may heighten the fee you have to pay them in the future. It already happened that somebody was kicked out of his insurance policy on grounds of fraud, because he was seen at a drag race on Facebook, and his application form didn't say he attended such events.

Banks

When you go to a bank to get credit the bank may also look at your online patterns to determine how large the risk is you wont be paying them back, similarly to how this already happens with [[insurance companies]].

Employment Agencies

Tracking data can also be useful with employment. An employer may want to know more about you and ask a company to generate a report about your online behaviour. At the moment there isn't any employment agency known to do this. Some people are already forced to reveal what is on their Facebook accounts, when they are at a job interview.

Rogue Employees

An employee from a perfectly behaving company, that is tracking you, may decide to sell data to interested companies for some extra money or misuse data in some other way. As far as is known, this never happened to tracking companies, but a Google employee has harassed teens by using online data once. More recently credit card numbers were sold by a T-Mobile employee to others.

Many More Possibilities

People running political campaigns may be interested in what you think is important to present you a digital pamphlet that addresses all those issues you're worried about. Burglars may pick up on travel plans together with your address. The list of possible ways to make money from online tracking is long and I'm sure there are uses people haven't even thought about.

GOOD REASONS TO TRACK PEOPLE

Machine Learning At Google

In the beginning of Google Search there was no spelling correction. Back then people would behave predictably, because when they made a spelling mistake and the results were off, they would correct themselves and immediately search again with the right spelling. As soon as Google started to track and record what people were searching for it must have been obvious that people searching for 'througj' afterwards searched for 'through'. The amount of people that did this could have been in the hundred thousands. Probably from that moment on Google's computers were told to suggest another spelling whenever somebody was searching for a word that 1) wasn't in the dictionary and 2) was often followed by a search for a word that was

in the dictionary. The functioning of Google's spelling correction is more complicated than how I describe it here, but the principle I touch upon holds up. The behavior of many thousands, up to many millions, of people have showed computers what correct and incorrect spelling is. Adding manually all possible spelling mistakes would be super inefficient in comparison to letting a computer â learnâ by allowing it to watch humans.

Machine Learning Should Be Anonymous

Important for my argument is that with machine learning it is unnecessary to know who exactly did what. It's for example unimportant to know who made the spelling mistakes where Google's computers have learned from. The â wisdomâ of the computer is created because many people made the mistake, not because a specific person X did it. Identity just doesn't matter for machine learning.

[[[necessary??]]]

Saving some sort of identity like IP addresses or cookies are non-functional while at the same time they can hold risks for the people who are making the mistakes. The search phrase data may matter to employers who want to have a fast way to check whether an applicant for a job is capable of spelling really good and types carefully. Leaked data from Google may indicate this to the employers, who are willing to pay a small price for the comfort of knowing somebody is good or not.

Science

The information that gets collected when people are tracked online may be valuable to sociologists or other scientists. An example where the availability of sensitive data to scientist have helped society happened in the previous century. When information about American citizens and house mortgage loans were combined it was shown that black people had to pay more for their house if they wanted to live in a white neighborhood, compared to the white people already living there. When this discrimination was proven by scientists the American government made legislation to make this an illegal practice.

Data Journalism

When a Republican was mentioned by name in any kind of message on Facebook (including private messages) the â moodâ of that message would be measured. This happened probably by counting the amount of positive and negative words in the message. This â moodâ indicator would in turn say something about how the elections for any Republican candidate were going. Such an application of information gathered from people is not nearly as useful as fighting discrimination in my opinion, but it remains a fact that good may come from using the data.

The way in which people are informed about the use and a meaningful possibility to withdraw your data from analysis could make practices like this acceptable. In the case of Facebook these conditions were not met unfortunately. Something that Facebook did correctly in my view was making sure that the political website only received the â moodâ indicators without knowing who was responsible for which â moodâ . Again it is irrelevant who said what exactly.

Application Programming Interface

When you use Google, either by typing search terms in the browsers address bar or by typing them on Google directly you are interacting with Google. The address bar and search bar through which you are interacting with Google are called an interface.

An Application Programming Interface is a means to interface with an â applicationâ in a different way than you're used to. You have to see application in a very broad sense. Google, Facebook and Twitter are considered web applications, but an organised set of data can be called a database application. Whatever the application is an Application Programming Interface (API) allows programmers to use that application in an automated way. By using the Google API a programmer could automatically search every word of an article in combination with the writer of that article. The program could then tell by looking at the amount of results it gets how often the author has used that word on the web. If you would leave out very common words this may result in an idea about the vocabulary of that author.

Similarly API's created for specific sets of data that are gathered by tracking people could be made available. Of course the data should be made anonymous before it is made available like this. At the moment too few people are knowledgeable about the possibilities of interfacing through an API to make the anonymous process and developing of a save API worthwhile. The highest risk for such an API would be that people are re-identified. If an API for an application that tracks grocery shopping habits is made available and name and address are obscured, but peoples general location is not, then there is a good change that the databases of delivery companies are capable to match the weight of delivered packages with groceries done. Since those delivery companies are sure to save your name and address the patterns of doing groceries and the patterns of delivered packages will together reveal who you are.

Attention Economy

Another reason why tracking is a good idea is to give marketers and content providers an idea about what is popular and what not. Marketers and content providers always try to predict what is popular and which part of a website will draw enough visitors. Sometimes however they are wrong in their estimates and it is a good thing that the professionals can then adjust their strategies and serve the public better. It would be a bad thing if things that people often come back for are hard to find while things that are almost never clicked are very prominent on the front page of a website. That's bad news for all parties.

Through similar methods people could be tracking you on their blog. This is good for people who are writing that block, because they can go to employers with actual data and say: â Look I attract so many people on this subject, take me as a content creator or expert on the topic.â

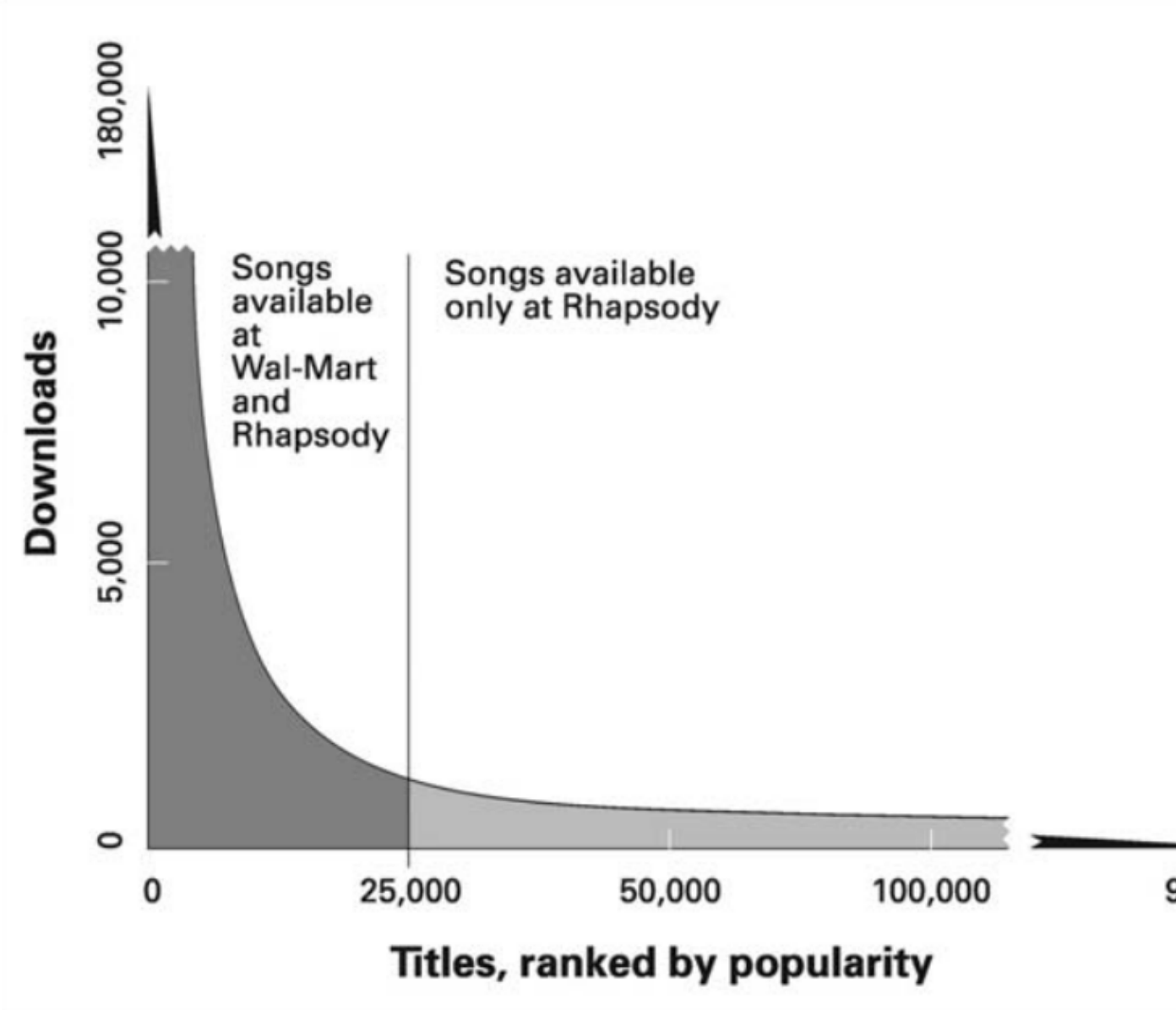
BAD REASONS TO TRACK PEOPLE

Demystifying The User Experience

A lot of advertising companies say they track people to deliver more interesting advertisements. I agree that [[some technologies add to the user experience]], but in nature they are completely different from advertising technologies. The major difference is that the former technologies, which are used in long-tail markets, have no need to identify you.

Hit And Long Tail Markets

Chris Anderson, a wired journalist, makes a distinction between hit and long-tail products. The term hit comes from music hits. Just like Madonna sells large quantities of music to people, so are there some products like Coca Cola who sell very good. Long-tail products are not very popular and do not sell very well, but because there are so many more long-tail products than hit products they all together bring more money in, than the hit products combined.



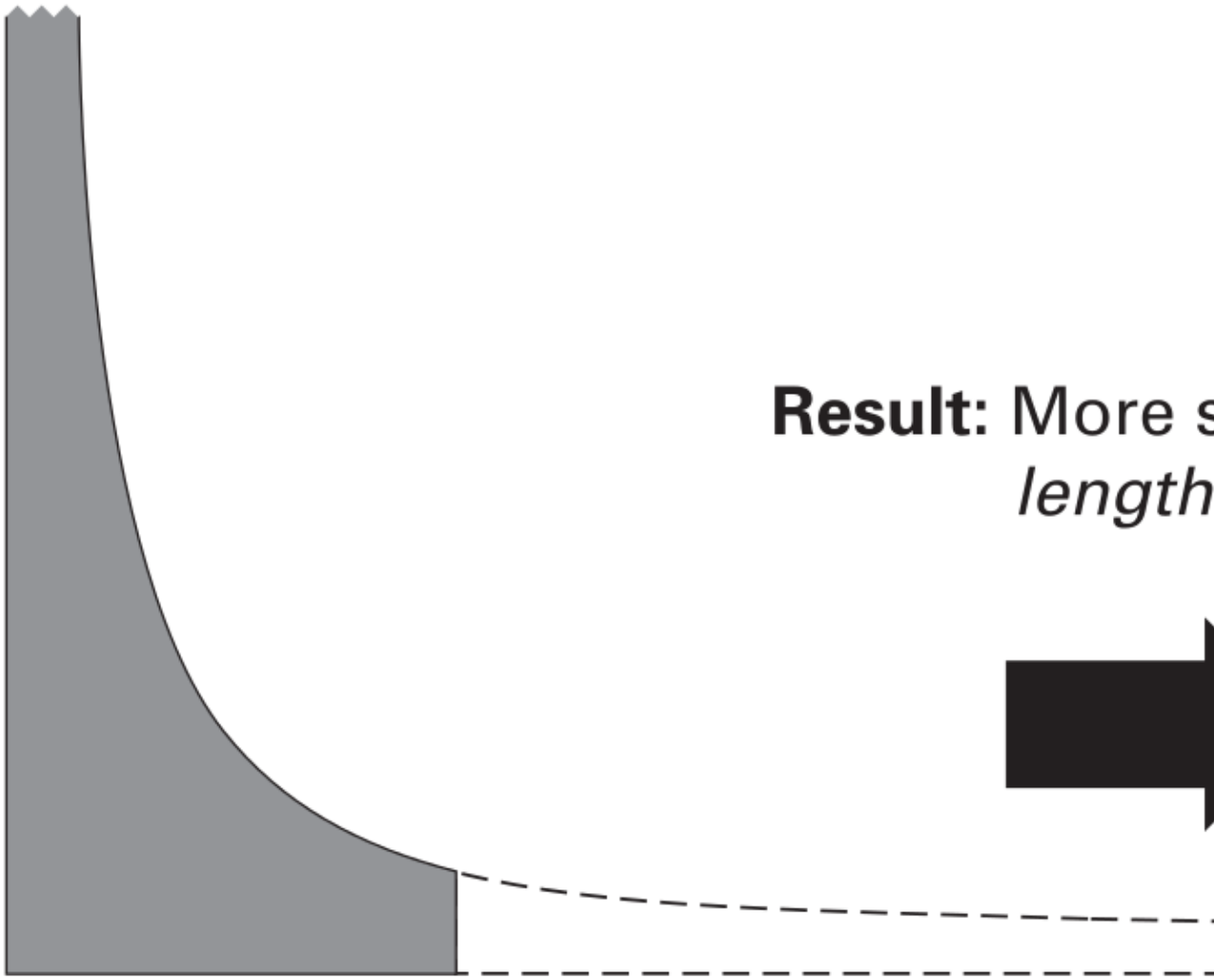
The image illustrates how a music market may look like in a graph. On the left side we see the hits (or head) market where a limited amount of songs is sold often. On the right side we see the tail market, where a lot of songs are sold, but not as regular as the hits. The tail is actually nine times longer than what we see in the graph now!

Examples Of Long Tail Companies

Companies like Amazon and Rhapsody are delivering an interesting user experience. They introduce people to new things they like, while at the same time they make things available you won't find in traditional shops and they are accessible from your home. However they don't need to identify you to deliver that experience. Unfortunately they may be tracking you even though there is no need for them to do so.

Making A Longer Tail

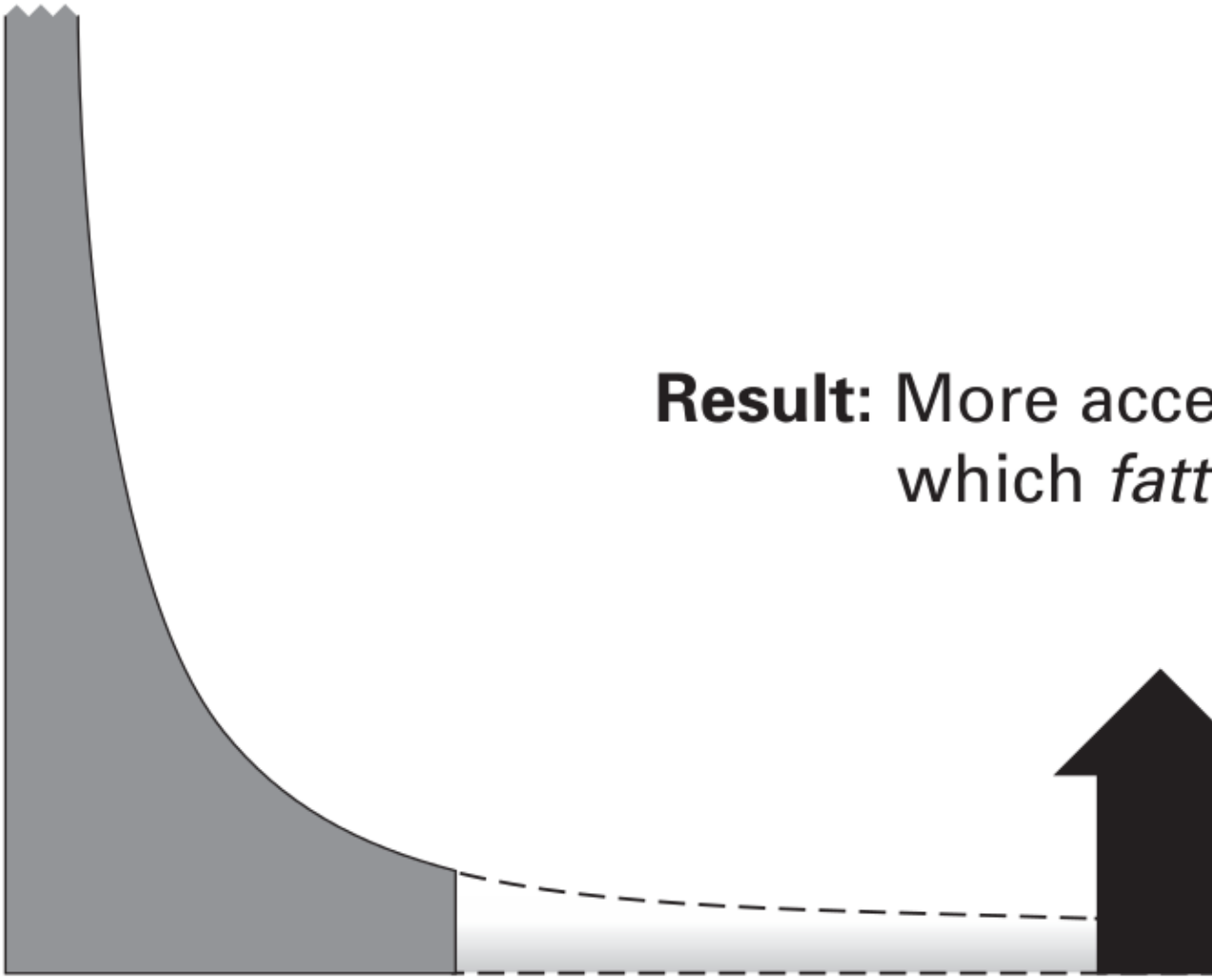
Practically everything can be made available online. There is no issue with this because the costs for making anything available to the masses is very low, and can be considered zero in many cases. Having more products available makes the tail in the long-tail market longer. This doesn't only add to the profit, because more products get sold. It also adds to the user experience, because with a larger assortment, you are more likely to run into something you really love.



Create Access To The Tail

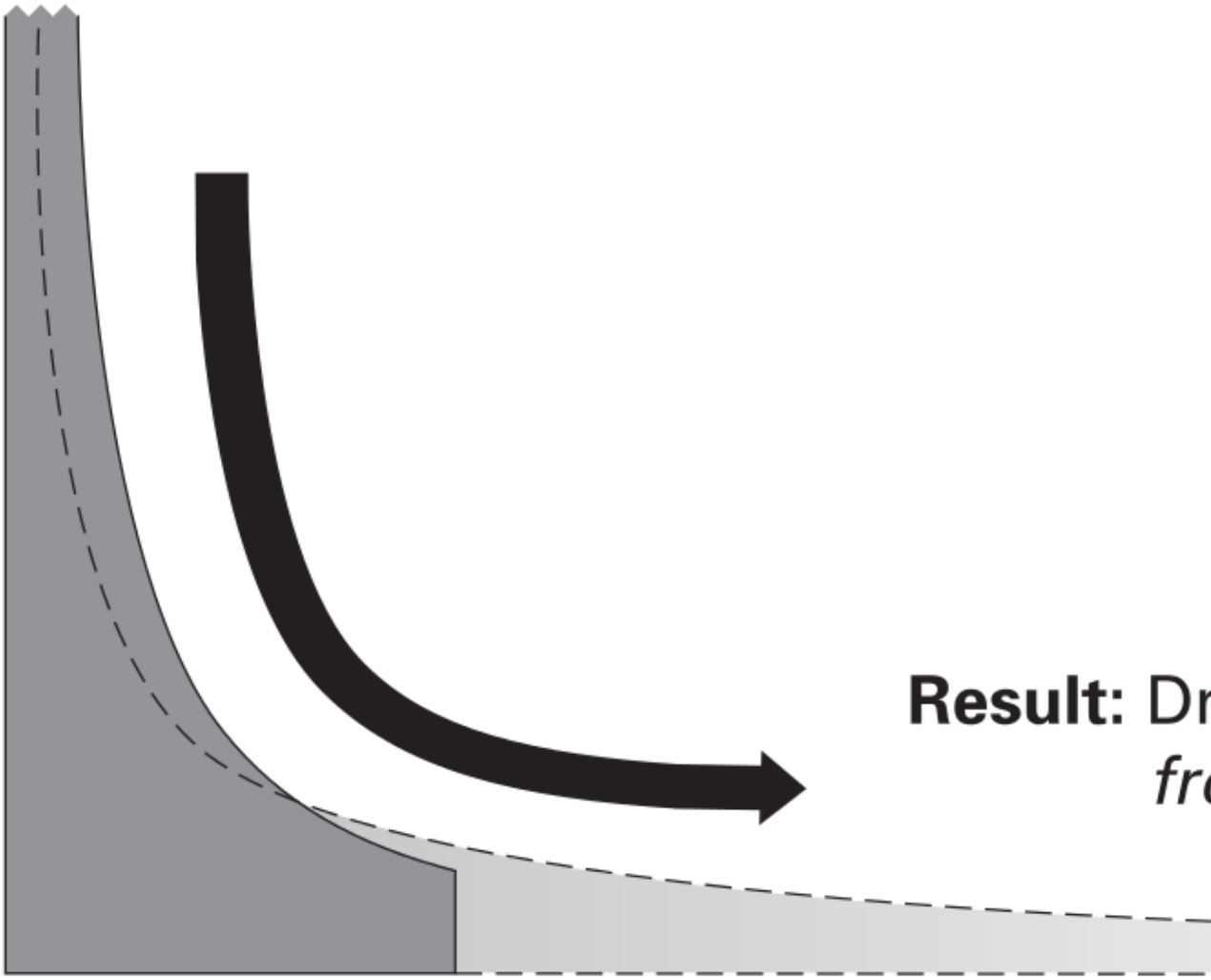
The easier people can find their way to products in the tail, the more profit a long-tail company makes and the better the user experience. With a digital platform consumers can find their way to products more easily than when people have to travel to get to a small shop somewhere. From the comfort of their homes, people are

more likely to have a pleasant experience and may buy more. A digital platform makes the tail of the market thicker.



Filtering The Tail

As computer algorithms learn what people like the products you like in the tail will get filtered from the things you hate. Through these filters the things that interest you in the tail will be as visible as the hits we all know. This will persuade consumers from the hit section to buy in the tail section. From a user point of view a filter has the power to introduce people to new things they probably like.



How Targeted Advertisement Works

Lets say that company A is interested in doing an online targeted advertisement campaign for product X. Furthermore lets assume that A goes to company B to achieve this, which is a targeting advertisement company. Company A will have an idea about their target group for product X. However, company C offers a product Y, which has the same target group. Company A and C now have to bid against each other on the site of company B. Company B will place the ad of the winner, whenever they see that the browser of somebody from the target group is requesting commercials as a webpage part from the server of company B.

Sometimes the same kind of bidding happens not on target group, but on search term. A search term is the phrase people enter in for instance Google when they are searching for something online. If I search for shoe, then some company may have bought a place between the advertisements I see, purely based on the search term I used.

A Different Realm

Targeted advertising always has to do with a limited amount of suppliers. If all suppliers would automatically have an advertisement place, why would advertisers pay for it? Advertisement agencies make money, because it only allows those who pay. Therefore they limit the amount of products, which goes against the good user experience of the long-tail. In fact any commercial you see online is likely to be for a hit product asking for more attention, because only those products !individually acquire enough money to justify an investment in advertisement. Targeted advertisement works with bidding and the price for an ad can be low if few companies bid for a certain search term. The problem with this is that it is then necessary to buy very specific search term like: â yellow green sportive shoes rotterdamâ . Using such search terms partially defeats the purpose of advertising, because your product will likely already be high in the results when a consumer is writing down such a specific search in a search engine.

Failure To Deliver A Good User Experience By Google

There are clear indicators that targeted advertising is in a completely different realm than the user friendly experience we have with long-tail platforms. This suspicion is confirmed when you look at the click-through-rate of commercials on Google. This percentage stands for the amount people that have clicked on an ad to read more about it. The average click-through-rate of Google is a shaming 2%. If only 2% of the users is interested in it I wouldn't dare to call it a user experience success. You may wonder how Google is able to make a profit with such a low success rate. The answer is scale. Google is showing those commercials to so many people that 2% ends up being a lot of people clicking it.

Retargeting And Use Experience

Another category of online advertisements are the retargeting ads. These ads will appear when a computer thinks you were about to buy shoes, but eventually didn't. I don't think this kind of advertisement can even be considered to be user friendly. For whatever reason the visitor decided not to buy, the change is not very big that the visitor completely forgot about the product and is grateful for the reminder.

Successes Are Biased

I can imagine that commercials on highly specialized technical blogs are considered to be an improvement instead of just a commercial by the visitors. The technological specifications of a device are very specialized and usually a lot of jargon is involved with these products. If somebody is visiting a webpage that contains this jargon or refers to specifications I can imagine that users mistake targeted advertisements for content as Anderson describes in his book. However a few successful anecdotes doesn't make the whole industry a user experience success. The problem is that technological products for hobby use are a very biased category. What about shoes? Shoes don't have a clear jargon and clear specifications which makes targeting advertisement in technological categories a success.

[[[Social advertising missing??]]]

PAYING WITH PRIVACY

No Such Thing As A Free Lunch

Contrary to popular believe a lot of things online are not free. Distribution online has become so cheap that a lot of companies will not charge you for the costs, making it appear as if it is free. These costs are so low,

because every year computational power, digital storage and the costs for sending digital information over a network have halved or more than halved every year for the last decades. A problem is that to buy these resources cheaply you'll have to buy a lot. You can get a transistor (a measure for computational power) for 0.000015 cents a piece, but only if you buy two billion at a time. If you want to buy one they are a dollar a piece. This means that if you want to provide your customers with free computing power like a free search algorithm that needs a lot of computation power, you'll have to invest greatly. Google spends hundreds of millions of dollars per year on equipment[[[source??]]]. The reason why we can use Google for free is that so many people use it that the cost per person is so close to zero, it isn't profitable to collect it. However the hundreds of millions have to come from somewhere.

Advertisement Cross Subsidy

The equipment used to deliver web services is payed for with advertisement income. In many cases advertisements pay completely or partially for services. Magazines cost a lot more to produce than the income a magazine gets from subscribers. Advertisement covers the rest of the costs. There is nothing wrong with this model and the money earned with it is estimated to be around 300 billion a year. For this model of financing the web tracking is unnecessary.

Google CEO Eric Schmidt is estimating that the market for targeted advertising is 800 billion. For targeted advertising online tracking is a necessity, because if you're not tracked, you can't possibly be targeted. In this kind of model we pay not only by seeing ads, but by giving up our privacy as well.

Freemium

A model that could support free web services without the need for tracking is a variant upon the freemium model, which is described by Chris Anderson. In this model 5% of the users support the rest of users. There are two products, one is free for all and for the other users have to pay a price, but that version works better in some way than the free version. It turns out that about 5% of the users will be using the advanced non free version. If this version is priced in such a way that a profit can be made for the entire product, then effectively 5% of the users is supporting a free version for the other 95%. Often this model works because some people have more time than money while others have more money than time. In a game for instance, where you have to travel in the game world, people are offered to buy teleportation stones. These â magicâ stones, which you can buy in an online shop, will get you anywhere in the game in an instance. If you would walk there it could take up to 10 minutes. Some people want to save time and buy stones, while some want to save money and spend time. A lot more people will spend time, but when the price of stones and products are correct the game can make a profit through it. Google could make everybody wait ten seconds unless they are a paying user. The people paying would also pay the equipment for users that do have to wait for their results.

Similarly Google could have people pay for guaranteed search privacy, while others make use of a non-free version where you give up your privacy. The question is whether privacy could not be worth a lot more than advertisement companies are currently willing to pay for it.

The Value Of Privacy

There are a few reasons why the loss of our privacy could cost us a lot of money, yet we are giving it away for free, while 3rd parties are earning billions with it. Google is paying some people a few dollars to loose their privacy, but this has not become practice for the masses. That's strange, because even though the distribution of tracking cookies to 3rd parties is virtually costless the information is rare and gets monetized. That should raise the price for this information considerably higher than free or only a few dollars! Big media companies are in full legal warfare to make money from their rare content like films and music. I think that it is waiting

for a solution for the masses to monetize their rare content somehow. I see opportunities at the level of tracking cookies and web beacons, because they are under control of the user.